

Tight finite-key analysis for passive decoy-state quantum key distribution under general attacks

Chun Zhou,^{1,3} Wan-Su Bao,^{1,3,*} Hong-Wei Li,^{1,2,3} Yang Wang,^{1,3}
Yuan Li,^{1,3} Zhen-Qiang Yin,^{2,3} Wei Chen,^{2,3} and Zheng-Fu Han^{2,3}

¹Zhengzhou Information Science and Technology Institute, Zhengzhou, 450004, China

²Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, 230026, China

³Synergetic Innovation Center of Quantum Information and Quantum Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China

(Dated: June 3, 2014)

For quantum key distribution (QKD) using spontaneous parametric-down-conversion sources (SPDCSs), the passive decoy-state protocol has been proved to be efficiently close to the theoretical limit of an infinite decoy-state protocol. In this paper, we apply a tight finite-key analysis for the passive decoy-state QKD using SPDCSs. Combining the security bound based on the uncertainty principle with the passive decoy-state protocol, a concise and stringent formula for calculating the key generation rate for QKD using SPDCSs is presented. The simulation shows that the secure distance under our formula can reach up to 182 km when the number of sifted data is 10^{10} . Our results also indicate that, under the same deviation of statistical fluctuation due to finite-size effects, the passive decoy-state QKD with SPDCSs can perform as well as the active decoy-state QKD with a weak coherent source.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) allows two legal communication parties to acquire the identical key based on quantum mechanics. Since the invention of the first pioneer QKD protocol, BB84 protocol [1], people have achieved great progress both in QKD's theory and experiment [2–9]. On the way toward the industrialization of QKD, people have faced sorts of obstacles, one of which comes from the fact that the necessary assumptions required for QKD's unconditional security are not easy to satisfy in a real situation [10]. Practical factors, i.e., inefficient authentication of classical communication, imperfections of setups and finite-size data, will undoubtedly threaten the security of a real QKD system and quantum hacking strategies can be successfully derived to attack the practical QKD system [11–13]. However, corresponding countermeasures can be applied to combat these attacks. One approach is to employ the notion of device-independent QKD (DI-QKD) [14–21]. The other, although difficult to implement, is to mathematically characterize the impact of imperfect factors on QKD's security as comprehensively as possible by a security proof [10].

The notion of finite-length keys is one of practical imperfections need to be solved in the practical security of QKD. In the case of finite-length keys, the security bound in the asymptotic regime should be reconsidered, and several attempts have been made to tackle this problem [22–26]. In recent years, based on the composable security definition derived from trace distance [27], several

significant advances have been achieved [28–34], with the most pioneering one being the bound from the smooth min-entropy by Scarani and Renner [29]. By noting that the uncertainty relation can be generalized to one formulated in terms of smooth entropies and that this directly implies the security of QKD protocols [4], Tomamichel et al. [35] creatively introduced the entropic formulation of the uncertainty relation into the security analysis of finite-length keys. Since then, many attempts were made to improve the security bound of finite resources, such as the situations for permutation-invariant protocols under coherent attacks [36], active decoy-state QKD [37], measurement-device-independent QKD [38], one-sided device-independent QKD [39], and the B92 protocol [40]. It should be noted that, by applying generalized chain rules for smooth min-entropies [41], information leakage from multiphoton pulses and vacuum pulses that the eavesdropper may exploit can be well bounded [37]. Thus, the result of Ref. [35] can be applied to most real situations when practical photon sources are used, e.g., weak coherent sources (WCSs) and spontaneous-parametric-down-conversion sources (SPDCSs).

SPDCS, like the commonly used WCSs, is also within reach of current technology and can be considered as another candidate of the perfect single photon source. However, due to the multiphoton fraction, QKD using SPDCSs is also vulnerable to the photon-number-splitting attack [42]. The active decoy-state method [43–45], i.e., actively and randomly varying the intensity of each signal state by a variable optical attenuator (VOA), can be conducted to combat this attack. But in some cases the imperfections of VOA might cause some physical parameters to rely on the particular setting selected and then threaten QKD's security [46]. Thus, passive preparation of intensity might be desirable in practice, and the

*Electronic address: 2010thzz@sina.com

first passive decoy-state protocol was presented by introducing a photon number resolving detector [47]. Then, Adachi et al. [48] presented an efficient passive decoy-state proposal (AYKI protocol) which can be easily realized with a practical threshold detector. More importantly, it is proved to be efficient enough for estimating the contribution of the single-photon pulse. Later, Ma and Lo [49] generalized the results of Refs. [48] and [47] to the most common case and Curty et al. [50] proposed a new passive decoy-state scheme for QKD using WCSs by subtly fitting a beam splitter with a threshold detector for triggering. However, all of the above results regarding the passive decoy-state scheme are obtained in the condition of asymptotic infinite-length keys. An effort to derive the security bound for the passive decoy-state method under finite resources has been made by Tan and Cai [51]. Their work is based on an indirect approach of tracing coherent attacks to collective attacks by the de Finetti theorem [52]. And for the direct approach based on the uncertainty principle [35], how the finite-size effect influences the performance of a passive decoy-state protocol needs further studying. This is just what we intend to clarify here.

In this paper, we directly introduce the formula of key generation rate obtained from Ref. [37] into the cases for passive decoy-state protocol. The difference is in the parameter estimation step, i.e., the way to estimate the single-photon yield and error rate in the scenario of finite-length keys. The starting point of the passive decoy-state protocol under asymptotic infinite-length keys is that the yield and bit error rate of the n -photon states from the triggered pulses are both equal to that from the nontriggered pulses. But this condition is no longer true under the condition of finite-length keys due to statistical fluctuations. Hence, we shall reconsider the steps of a passive decoy-state protocol for estimating single-photon yield and error rate. Luckily, it is found that the yield and bit error rate of n -photon states can be considered as random variables emanating from sampling without replacement. Then, by applying the Serfling bound [53] in sample theory, one can construct confidence regions of the interval estimate for these variables, which was first introduced into the parameter estimation of QKD by Scarani et al. [29] and then improved by Tomamichel et al. [35] and Mertz et al. [36]. Thus, in the confidence regions, there certainly exist relationships for the parameters between triggered events and nontriggered events, which can be directly applied to estimate the gain and bit error rate of triggered and non-triggered single-photon events, respectively. In particular, without relying on any approximation, we introduce a rigorous method based on a hypergeometric argument [33] to bound the quantity of the maximal information of an eavesdropper on the single-photon events. Note that our security analysis is conducted based on the uncertainty principle and that bound in [33] holds true under no approximation; thus the formulas we obtain are valid for general coherent attacks and our results guarantee unconditional security.

We compare our results with those derived from active decoy protocol [37] and the simulations show the efficiency of our protocol.

The paper is organized as follows. In Sec. II, we fix the security preliminaries, clarify the formalism used to calculate secret key rates under the assumption of general attacks and introduce the bound for estimating the phase error rate in our protocol. Section III recalls the AYKI protocol for QKD with asymptotic infinite-length keys. The main results of this paper, i.e., tight formulas for estimating the yield and bit error rate for single-photon events, are presented in Sec. IV. Section V numerically simulates our results and Sec. VI concludes the paper.

II. SECURITY CRITERIA AND SMOOTH MIN-ENTROPY

In this paper we consider an asymmetric coding BB84 protocol, where the bases X and Z are chosen with probabilities q_X and q_Z that are biased. The protocol consists of these steps: state preparation, state measurement, sifting, parameter estimation (PE), error correction (EC), error verification, and privacy amplification (PA) (for a detailed description, see Ref. [37]). The protocol outputs are S_A and S_B on Alice's and Bob's side respectively. Only and only if successfully passing all of the above steps can S_A and S_B be considered secure. Here, the security criterion based on trace distance, seminally proposed by Renner, is introduced in our analysis [27]:

Definition 1 (composable security definition). Assume a QKD protocol outputs keys of S_A and S_B on Alice's and Bob's side respectively. It is considered to be ε -secure if it satisfies both the correctness and the secrecy. Correctness means that the protocol is ε_{cor} -correct if $P(S_A \neq S_B) \leq \varepsilon_{\text{cor}}$, namely the probability of $S_A \neq S_B$ will not exceed ε_{cor} . Secrecy means that the protocol is ε_{sec} -secret if $\frac{p_{\text{pass}}}{2} \|\rho_{SE} - U_S \otimes \rho_E\|_1 \leq \varepsilon_{\text{sec}}$ where S represents either of the keys S_A and S_B , ρ_E is the system that the eavesdropper owns, ρ_{SE} is the classical-quantum state describing the joint state of S and E , U_S is the uniform mixture of all possible values of S , and p_{pass} is the probability that all steps of the protocol are successfully conducted.

Smooth min-entropy, relying on a generalization of the von Neumann entropy, is an essential tool in the security proof based on information theory [27]. Combined with the uncertainty principle, it directly implies a security proof without the assumption that the measurement devices work according to the specifications of the protocol [4]. In particular, it can provide us an efficient method for the finite-key analysis [35]. If we denote \mathcal{H} as a finite dimensional Hilbert space and let $\mathcal{P}(\mathcal{H})$ be the set of positive semidefinite operators on \mathcal{H} . Then, the set of normalized quantum states and subnormalized ones can be presented by $\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \text{tr} \rho = 1\}$ and $\mathcal{S}_{\leq}(\mathcal{H}) := \{\rho \in \mathcal{P}(\mathcal{H}) : \text{tr} \rho \leq 1\}$, respectively. Given these, the definition of smooth min-entropy can be defined

as the following[27]:

Definition 2 (smooth min-entropy). Let $\varepsilon \geq 0$, $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$ and $\rho_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB})$. The smooth min-entropy $H_{\min}^{\varepsilon}(A|B)$, taken over a set of states $\mathcal{B}^{\varepsilon}(\rho)$ that are ε -close to ρ_{AB} , is defined as the quantity

$$\max_{\tilde{\rho} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} \{-\log_2 \min\{\lambda > 0 : \exists \sigma_B : \tilde{\rho}_{AB} \leq \lambda \text{id}_A \otimes \sigma_B\}\}, \quad (1)$$

where $\mathcal{B}^{\varepsilon}(\rho) := \{\tilde{\rho}_{AB} \in \mathcal{S}_{\leq}(\mathcal{H}_{AB}) : C(\rho_{AB}, \tilde{\rho}_{AB}) \leq \varepsilon\}$, id_A is the identity operator on A , $C(\rho_{AB}, \tilde{\rho}_{AB}) := 1 - (\text{tr}|\sqrt{\rho}\sqrt{\tilde{\rho}}|)^{2^{1/2}}$ is a distance measure based on fidelity and ε is called the smoothing parameter.

There exists the following chain rule for the smooth min-entropy[41, 54]:

Lemma 1 (Chain-rule inequality for the smooth min-entropy). Let $\varepsilon \geq 0$, $\varepsilon', \varepsilon'' \geq 0$, and $\rho_{ABC} \in \mathcal{S}_{\leq}(\mathcal{H}_{ABC})$. Then

$$H_{\min}^{\varepsilon+\varepsilon'+2\varepsilon''}(AB|C)_{\rho} \geq H_{\min}^{\varepsilon''}(A|BC)_{\rho} + H_{\min}^{\varepsilon'}(B|C)_{\rho} - f(\varepsilon), \quad (2)$$

where $f(\varepsilon) = \log_2 \frac{1}{1-\sqrt{1-\varepsilon^2}}$.

Let system E' be the information that Eve obtains on the raw key X_A of Alice, prior to the error-verification step. Then, after the privacy amplification step, the length of the secure key S_A can be expressed by the following lemma.

Lemma 2 (Secret key based on smooth min-entropy) [27, 37]: By applying privacy amplification with two-universal hashing, a secret key extracted from X_A is ε_{sec} -secret if its length ℓ is chosen such that

$$\lfloor H_{\min}^{\nu}(X_A|E') - 2\log_2 \frac{1}{2^{\bar{\nu}}} \rfloor, \quad (3)$$

where $\nu + \bar{\nu} \leq \varepsilon_{\text{sec}}$ with ν and $\bar{\nu}$ chosen to be proportional to $\frac{\varepsilon_{\text{sec}}}{p_{\text{pass}}}$, and $H_{\min}^{\nu}(X_A|E')$ quantifies the amount of uncertainty system E has on X_A .

III. AYKI PROTOCOL WITH INFINITE-LENGTH KEYS

In the AYKI protocol, two-mode states are prerequisite and we consider those emitted from the nondegenerate spontaneous-parametric-down-conversion (SPDC) process. This type of SPDC processes creates the two-mode state [55]

$$(\cosh \chi)^{-1} \sum_{n=0}^{\infty} (\tanh \chi)^n e^{in\theta} |n, n\rangle. \quad (4)$$

Set the intensity μ of the source to $\sinh^2 \chi$, then the above description simplifies to

$$\sum_{n=0}^{\infty} \sqrt{\frac{\mu^n}{(1+\mu)^{n+1}}} e^{in\theta} |n, n\rangle \quad (5)$$

When the sender (Alice) measures one mode of her states from the above SPDCS with a practical threshold

detector described by detection efficiency η_A and dark-count rate d_A , the other mode can be divided into two parts according to the response of the threshold detector, i.e., the triggered events and nontriggered events. Both of them are sent to the lossy channel, detected by the receiver's (Bob's) detector and devoted to the final secret key. In particular, the nontriggered events, acting as the role of decoy states, can be used to estimate the single-photon contribution and single-photon error.

In this case, the signal n -photon events with probability p_n are also divided into two parts, the triggered n -photon events with probability of $p_n^{(t)}$ and the nontriggered n -photon events with probability of $p_n^{(\text{nt})}$. Let γ_n be the probability of detection (triggering) when n photons are emitted from the SPDC process. Then, $p_n^{(t)} = p_n \gamma_n$ and $p_n^{(\text{nt})} = p_n(1 - \gamma_n)$ with [48]

$$p_n = \frac{\mu^n}{(1+\mu)^{n+1}}, \quad \gamma_n = 1 - (1 - d_A)(1 - \eta_A)^n. \quad (6)$$

In this paper, we consider the measurement model mentioned in Ref. [48]. It should be noted that, in the case of asymptotic infinite-length keys, it is assumed that the detection rate (yield) and quantum bit error rate (QBER) of the triggered n -photon events are the same as those of the nontriggered n -photon events, i.e.,

$$Y_n^{(t)} = Y_n^{(\text{nt})}, \quad e_n^{(t)} = e_n^{(\text{nt})}. \quad (7)$$

Under this condition, it is not easy to find that [48]

$$Q_n^{(t)} = \delta_n Q_n^{(\text{nt})}, \quad (8)$$

where $Q_n^{(t)} = Y_n^{(t)} p_n \gamma_n$, $Q_n^{(\text{nt})} = Y_n^{(\text{nt})} p_n(1 - \gamma_n)$ and $\delta_n = \frac{\gamma_n}{1 - \gamma_n}$. Noting that $0 \leq \delta_0 < \delta_1 < \delta_2 < \dots$ and considering the overall detection rate $Q^{(t)} = \sum_{n=0}^{\infty} Q_n^{(t)}$ with triggering and $Q^{(\text{nt})} = \sum_{n=0}^{\infty} Q_n^{(\text{nt})}$ without triggering, one can obtain a lower bound for the single-photon detection rate $Q_1^{(\text{nt})}$ without triggering [48]:

$$Q_1^{(\text{nt})} \geq \frac{(\delta_2 - \delta)Q^{(\text{nt})} - (\delta_2 - \delta_0)Q_0^{(\text{nt})}}{\delta_2 - \delta_1} \triangleq \xi(Q_0^{(\text{nt})}), \quad (9)$$

where $\delta = \frac{Q^{(t)}}{Q^{(\text{nt})}}$. Then, taking the overall QBER $E^{(t)} = \sum_{n=0}^{\infty} \frac{Q_n^{(t)} e_n^{(t)}}{Q^{(t)}}$ with triggering and the one $E^{(\text{nt})} = \sum_{n=0}^{\infty} \frac{Q_n^{(\text{nt})} e_n^{(\text{nt})}}{Q^{(\text{nt})}}$ without triggering into account, one can derive an upper bound for the single-photon error rate [48]:

$$e_1 \leq \min\left(\frac{2\delta E^{(t)} Q^{(\text{nt})} - \delta_0 Q_0^{(\text{nt})}}{2\delta_1 \xi(Q_0^{(\text{nt})})}, \frac{2E^{(\text{nt})} Q^{(\text{nt})} - Q_0^{(\text{nt})}}{2\xi(Q_0^{(\text{nt})})}\right) \triangleq \epsilon(Q_0^{(\text{nt})}), \quad (10)$$

where $0 \leq Q_0^{(\text{nt})} \leq \min(2E^{(t)} Q^{(\text{nt})}(\delta/\delta_0), 2E^{(\text{nt})} Q^{(\text{nt})})$.

Taking both of the keys derived from the triggered events and nontriggered events into consideration, and applying the GLLP formula [3], one can obtain the final key rate which is shown by Eqs.(13) and (14) in Ref. [48].

IV. PASSIVE DECOY-STATE PROTOCOL WITH FINITE-LENGTH KEYS

Due to the effect of finite-size data sets in real-life experiments, there exist various fluctuations in the parameter-estimation step [56]. For a SPDCS, it is proved that the AYKI protocol actually always holds with whatever intensity fluctuation of pump light [57]. Hence, in this paper, we mainly consider the influence of the finite-size effect on the estimation of single-photon yield, single-photon error rate, and phase error rate.

A. Phase error rate

Here, the phase errors, an argument arising from the Shor–Preskill formalism [2], means that the maximal virtual errors come from the activity of smart eavesdroppers. It can not be directly measured in experiment and, in the case of a finite-size data set, has to be estimated via a random-sampling theory according to the observed bit errors. In this paper, we apply the interval estimation based on the straightforward bounds [33] from an approaching technique for the hypergeometric distribution. It should be noted that this estimation is in accordance with the security criteria based on trace distance and, most importantly, is proved to be tighter than the one in Ref. [35] and more stringent than the one in Ref. [58].

Lemma 3 (straightforward bound). Let n , l and c be the sifted bits, sample bits and observed error bits, respectively. Suppose the final keys of the QKD protocol are ε_{sec} -secret, then their phase error rate e_p is given by [33]

$$e_p = \frac{(n+l)\hat{e}(c+2)-le_{\text{ob}}(c+2)}{n} \triangleq g(e_{\text{ob}}(c)), \quad (11)$$

with

$$\begin{aligned} \hat{e}(c) &= \frac{e_{\text{ob}}(c)+2\tau+2\sqrt{\tau\{e_{\text{ob}}(c)[1-e_{\text{ob}}(c)]+\tau\}}}{1+4\tau}, \\ \tau &= \frac{\omega^2 n}{4l(n+l-1)}, \\ e_{\text{ob}}(c) &= c/l, \end{aligned} \quad (12)$$

where ω is chosen satisfying

$$\sqrt{\frac{n+l}{n}} \sqrt{\frac{\omega^2+2\pi}{2}} e^\nu \Phi(\omega) \leq \frac{1}{16} \varepsilon_{\text{sec}}^2. \quad (13)$$

Here, $\nu = \frac{1}{6n} + \frac{1}{12}$ and $\Phi(\omega) = \frac{1}{\sqrt{2\pi}} \int_\omega^\infty \exp(-\frac{y^2}{2}) dy$.

B. single-photon yield

In the case of finite-length keys, the yield of the triggered n -photon events are no longer equal to that of the nontriggered ones, i.e.,

$$Y_n^{(t)} \neq Y_n^{(\text{nt})}. \quad (14)$$

However, by the theory of probability statistics, there certainly exist relations between the two parts in concrete confidence regions. This means, that the yield of the triggered n -photon events is ξ close to that of the nontriggered ones, which corresponds to the two parts being equal except with a probability of ϵ_n . Here, we consider the bound widely used in finite-key QKD and first introduce the following lemma into estimating the relation between the yields [35, 36]:

Lemma 4. Let $\epsilon_n > 0$ and $n_1, n_2 > 0$. Let ρ^{n_1} and ρ^{n_2} be the quantum state of the triggered and non-triggered n -photon events, respectively. They are both permutation-invariant quantum states, and let \mathcal{E} be a positive-operator-value measure (POVM) on \mathcal{H}_{AB} which outputs the yield and quantum bit error rate, where $\rho^{n_1+n_2} \in \mathcal{S}(\mathcal{H}_{AB}^{\otimes n_1+n_2})$. Let $\mathbf{Y}_n^{(t)}$ and $\mathbf{Y}_n^{(\text{nt})}$ be the frequency distribution of the measurement events, e.g., the yield, when applying the measurement \mathcal{E}^{n_1} and \mathcal{E}^{n_2} , respectively. Then, for any element $Y_n^{(t)}$ and $Y_n^{(\text{nt})}$ from $\mathbf{Y}_n^{(t)}$ and $\mathbf{Y}_n^{(\text{nt})}$ except with probability ϵ_n ,

$$\frac{1}{2} \| Y_n^{(t)} - Y_n^{(\text{nt})} \| \leq \xi(\epsilon_n, n_1, n_2), \quad (15)$$

with $\xi(\epsilon_n, n_1, n_2) = \sqrt{\frac{(n_1+n_2)(n_1+1)\ln(1/\epsilon_n)}{8n_1^2 n_2}}$, where n_1 and n_2 are the number of n -photon triggered events and n -photon nontriggered events, respectively, chosen for parameter estimation.

Note that the overall detection rate with triggering and without triggering are expressed respectively by

$$Q^{(t)} = \sum_{n=0}^{\infty} Q_n^{(t)} = \sum_{n=0}^{\infty} Y_n^{(t)} p_n \gamma_n, \quad (16)$$

$$Q^{(\text{nt})} = \sum_{n=0}^{\infty} Q_n^{(\text{nt})} = \sum_{n=0}^{\infty} Y_n^{(\text{nt})} p_n (1 - \gamma_n). \quad (17)$$

Equation (17) is multiplied by δ_2 and we obtain

$$\delta_2 Q^{(\text{nt})} = \delta_2 Q_0^{(\text{nt})} + \delta_2 Q_1^{(\text{nt})} + \delta_2 \sum_{k=2}^{\infty} Q_k^{(\text{nt})}. \quad (18)$$

From Eq.(15), we can find that $Y_n^{(\text{nt})} \leq Y_n^{(t)} + 2\xi_n$, where $\xi_n = \xi(\epsilon_n, n_1, n_2)$. Then, the third term of the right-hand side of the above equation satisfies

$$\begin{aligned} \delta_2 \sum_{k=2}^{\infty} Q_k^{(\text{nt})} &\leq \delta_2 \sum_{k=2}^{\infty} (Y_k^{(t)} + 2\xi_k) p_k (1 - \gamma_k) \\ &\leq \sum_{k=2}^{\infty} (Y_k^{(t)} + 2\xi_k) p_k \gamma_k \\ &= \sum_{k=2}^{\infty} Q_k^{(t)} + 2 \sum_{k=2}^{\infty} \xi_k p_k \gamma_k, \end{aligned} \quad (19)$$

where $\sum_{k=2}^{\infty} Q_k^{(t)} = Q^{(t)} - Q_0^{(t)} - Q_1^{(t)}$. Hence, from Eq.(17),

one can obtain

$$\begin{aligned}
& \delta_2(Q^{(\text{nt})} - Q_0^{(\text{nt})} - Q_1^{(\text{nt})}) \\
& \leq Q^{(t)} - Q_0^{(t)} - Q_1^{(t)} + 2 \sum_{k=2}^{\infty} \xi_k p_k \gamma_k \\
& \leq Q^{(t)} + (2\xi_1 - Y_1^{(\text{nt})})p_1\gamma_1 + (2\xi_0 - Y_0^{(\text{nt})})p_0\gamma_0 \\
& \quad + 2 \sum_{k=2}^{\infty} \xi_k p_k \gamma_k \\
& = Q^{(t)} - \delta_0 Q_0^{(\text{nt})} - \delta_1 Q_1^{(\text{nt})} + 2 \sum_{k=0}^{\infty} \xi_k p_k \gamma_k.
\end{aligned} \tag{20}$$

We thus obtain a minimum value of $Q_1^{(\text{nt})}$ as a function of $Q_0^{(\text{nt})}$:

$$Q_1^{(\text{nt})} \geq \frac{\delta_2 Q^{(\text{nt})} - Q^{(t)} - (\delta_2 - \delta_0)Q_0^{(\text{nt})} - 2 \sum_{k=0}^{\infty} \xi_k p_k \gamma_k}{\delta_2 - \delta_1}. \tag{21}$$

Let p_{pe} be the probability of choosing a pulse from the SPDC process as the sample bits used for parameter estimation. Then, if we assume $\epsilon_{\text{pe}} = \epsilon_0 = \epsilon_1 = \epsilon_2 = \dots$ and note that $k_1 = Np_{\text{pe}}p_k\gamma_k$ and $k_2 = Np_{\text{pe}}p_k(1 - \gamma_k)$ in $\xi_k = \xi(\epsilon_k, k_1, k_2)$, the above bound can be further represented by

$$\frac{Q_1^{(\text{nt})}}{Q^{(\text{nt})}} \geq \frac{[(\delta_2 - \delta) - (\delta_2 - \delta_0)x - \chi]}{\delta_2 - \delta_1} \triangleq \zeta(x), \tag{22}$$

where N denotes the number of total pulses emitted from the SPDC process, $x = \frac{Q_0^{(\text{nt})}}{Q^{(\text{nt})}}$ and $\chi = \frac{1}{Q^{(\text{nt})}} \sqrt{\frac{\ln(1/\epsilon_{\text{pe}})}{2Np_{\text{pe}}}} \sum_{k=0}^{\infty} \sqrt{\delta_k p_k}$. From Eq.(15), one can also find that $Y_1^{(t)} \geq Y_1^{(\text{nt})} - 2\xi_1$. Therefore, we can also obtain a lower bound for $Q_1^{(t)}$:

$$Q_1^{(t)} \geq \delta_1 Q_1^{(\text{nt})} - \chi_1 \geq \delta_1 Q^{(\text{nt})} \zeta(x) - \chi_1, \tag{23}$$

where $\chi_1 = \sqrt{\frac{\delta_1 p_1 \ln(1/\epsilon_{\text{pe}})}{2Np_{\text{pe}}}}$.

C. single-photon error rate

The overall quantum bit error rate for the triggered events and nontriggered events can be represented, respectively, by

$$Q^{(t)} E^{(t)} = \sum_{n=0}^{\infty} Q_n^{(t)} e_n^{(t)} = \sum_{n=0}^{\infty} Y_n^{(t)} e_n^{(t)} p_n \gamma_n, \tag{24}$$

$$Q^{(\text{nt})} E^{(\text{nt})} = \sum_{n=0}^{\infty} Q_n^{(\text{nt})} e_n^{(\text{nt})} = \sum_{n=0}^{\infty} Y_n^{(\text{nt})} e_n^{(\text{nt})} p_n (1 - \gamma_n). \tag{25}$$

From Eqs.(15), (23) and (24) with $e_0^{(t)} = \frac{1}{2}$, an upper bound on $e_1^{(t)}$ is given by

$$\begin{aligned}
e_1^{(t)} & \leq \frac{Q^{(t)} E^{(t)} - Q_0^{(t)} e_0^{(t)}}{Q_1^{(t)}} \leq \frac{2Q^{(t)} E^{(t)} - Q_0^{(t)}}{2(\delta_1 Q_1^{(\text{nt})} - \chi_1)} \\
& \leq \frac{2Q^{(t)} E^{(t)} - \delta_0 Q_0^{(\text{nt})} + \chi_0}{2[\delta_1 Q^{(\text{nt})} \zeta(x) - \chi_1]} \\
& \leq \frac{2\delta E^{(t)} - \delta_0 x + \chi_0 / Q^{(\text{nt})}}{2\delta_1 \zeta(x) - 2\chi_1 / Q^{(\text{nt})}} \triangleq \mathcal{W}_t(x),
\end{aligned} \tag{26}$$

where $\chi_0 = \sqrt{\frac{\delta_0 p_0 \ln(1/\epsilon_{\text{pe}})}{2Np_{\text{pe}}}}$.

Similarly, from Eqs.(15), (22) and (25) with $e_0^{(\text{nt})} = \frac{1}{2}$, one can have an upper bound on $e_1^{(\text{nt})}$, which is shown by

$$e_1^{(\text{nt})} \leq \frac{Q^{(\text{nt})} E^{(\text{nt})} - Q_0^{(\text{nt})} e_0^{(\text{nt})}}{Q_1^{(\text{nt})}} \leq \frac{2E^{(\text{nt})} - x}{2\zeta(x)} \triangleq \mathcal{W}_{\text{nt}}(x) \tag{27}$$

D. Secret key length

If we consider the secret key only from the triggered events and apply Lemma 2, a ϵ_{sec} -secret key of length ℓ can be given by

$$\lfloor H_{\min}^{\nu}(X_A^{(t)} | E') - 2 \log_2 \frac{1}{2^{\overline{\nu}}} \rfloor, \tag{28}$$

where $X_A^{(t)}$ is the raw key extracted from the triggered events, $\nu + \overline{\nu} \leq \epsilon_{\text{sec}}$ with ν and $\overline{\nu}$ chosen to be proportional to $\frac{\epsilon_{\text{sec}}}{p_{\text{pass}}}$.

Then, applying the results of Ref. [37], the length of secret key from the triggered events can be represented by

$$\lfloor n_0^{(t)} + n_1^{(t)}(1 - h(e_p^{(t)})) - \lambda_{EC}^{(t)} - 6 \log_2 \frac{10}{\epsilon_{\text{sec}}} - \log_2 \frac{2}{\epsilon_{\text{cor}}} \rfloor, \tag{29}$$

where $h(x) := -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function, $n_0^{(t)} \geq NQ^{(\text{nt})}(\delta_0 x - \frac{\chi_0}{Q^{(\text{nt})}})$ with $\chi_0 = \sqrt{\frac{\delta_0 p_0 \ln(1/\epsilon_{\text{pe}})}{2N}}$, $n_1^{(t)} \geq NQ^{(\text{nt})}[\delta_1 \zeta(x) - \frac{\chi_1}{Q^{(\text{nt})}}]$, $e_p^{(t)}$ denotes the phase error rate which is calculated by Lemma 3, $\lambda_{EC}^{(t)} = NQ^{(t)} f_{EC} h(E^{(t)})$. It should be noted that $\epsilon_{\text{sec}} = 9\epsilon + \epsilon_{\text{pe}}$ where ϵ_{pe} is the failure probability of estimating the single-photon yield and error rate mentioned in the previous subsection. Let $\epsilon_{\text{pe}} = \epsilon$, then $\epsilon_{\text{sec}} = 10\epsilon$, which is different from Ref. [37]. ϵ_{cor} is the security parameter of the error-verification step. Hence, the length of the secret key from the triggered events can be shown as

$$\begin{aligned}
\ell_T & = \min_x \{ N(1 - p_{\text{pe}})Q^{(\text{nt})}[\delta_0 x - \frac{\chi_0}{Q^{(\text{nt})}}] \\
& \quad + (\delta_1 \zeta(x) - \frac{\chi_1}{Q^{(\text{nt})}})(1 - h(e_p^{(t)})) \} \\
& \quad - N(1 - p_{\text{pe}})Q^{(t)} f_{EC} h(E^{(t)}) \\
& \quad - 6 \log_2 \frac{10}{\epsilon_{\text{sec}}} - \log_2 \frac{2}{\epsilon_{\text{cor}}},
\end{aligned} \tag{30}$$

where $\chi_i = \sqrt{\frac{\delta_i p_i \ln(1/\epsilon_{\text{pe}})}{2Np_{\text{pe}}}}$ with $i = 0$ or $i = 1$, p_{pe} is the probability of choosing a pulse from the SPDC process as the sample events used for parameter estimation and $e_p^{(t)} = g(\mathcal{W}_t(x))$. The minimum is numerically taken over the range $0 \leq x \leq \min\{2E^{(t)}/\delta_0, 2E^{(\text{nt})}\}$.

However, if we also take the secret key from the non-triggered events into account when the error reconciliation is separately applied to the triggered events and to the nontriggered events, but the privacy amplification is applied together, Eq.(28) no longer holds true and we shall recalculate the length of the secret key by

$$\lfloor H_{\min}^{\nu}(X_A^{(t)} X_A^{(\text{nt})} | E^{(t)'} E^{(\text{nt})'}) - 2 \log_2 \frac{1}{2^{\overline{\nu}}} \rfloor, \tag{31}$$

where $X_A^{(t)}$ and $X_A^{(nt)}$ are the raw key extracted from the triggered and nontriggered events respectively, $E^{(t)'}$ and $E^{(nt)'}$ are the information that Eve gathers on $X_A^{(t)}$ and $X_A^{(nt)}$, respectively, up to the error verification step. In the following, we will show how to estimate a lower bound of the left term in Eq.(31).

By Lemma 1, we have that

$$\begin{aligned} H_{\min}^{\nu}(X_A^{(t)} X_A^{(nt)} | E^{(t)'} E^{(nt)'}) \\ \geq H_{\min}^{\nu_2}(X_A^{(t)} | X_A^{(nt)} E^{(t)'} E^{(nt)'}) \\ + H_{\min}^{\nu_3}(X_A^{(nt)} | E^{(t)'} E^{(nt)'}) - f(\nu_1) \\ = H_{\min}^{\nu_2}(X_A^{(t)} | E^{(t)'}) + H_{\min}^{\nu_3}(X_A^{(nt)} | E^{(nt)'}) - f(\nu_1), \end{aligned} \quad (32)$$

where

$$\begin{aligned} f(\nu_1) &= \log_2(2/\nu_1^2), \\ \nu &= \nu_1 + 2\nu_2 + \nu_3, \\ H_{\min}^{\nu_2}(X_A^{(t)} | E^{(t)'}) &\geq H_{\min}^{\nu_2}(X_A^{(t)} | E^{(t)}) - \lambda_{EC}^{(t)} - \log_2(2/\varepsilon_{\text{cor}}), \\ H_{\min}^{\nu_3}(X_A^{(nt)} | E^{(nt)'}) &\geq H_{\min}^{\nu_3}(X_A^{(nt)} | E^{(nt)}) - \lambda_{EC}^{(nt)} - \log_2(2/\varepsilon_{\text{cor}}). \end{aligned} \quad (33)$$

In the above equations, $E^{(t)}$ and $E^{(nt)}$ denote the remaining quantum information that Eve has on $X_A^{(t)}$ and $X_A^{(nt)}$, respectively, after the error correction and error verification steps. According to the analysis of Ref. [37], the terms $H_{\min}^{\nu_2}(X_A^{(t)} | E^{(t)})$ and $H_{\min}^{\nu_3}(X_A^{(nt)} | E^{(nt)})$ in Eq.(33) can be lower bounded by the generalized chain-rule result (Lemma 1 [41]) and the uncertainty relation for smooth entropies [35]. Precisely, they are given by

$$\begin{aligned} H_{\min}^{\nu_2}(X_A^{(t)} | E^{(t)}) &\geq n_0^{(t)} + n_1^{(t)}(1 - h(e_p^{(t)})) - \log_2 \frac{2}{(\alpha_2 \alpha_3)^2}, \\ H_{\min}^{\nu_3}(X_A^{(nt)} | E^{(nt)}) &\geq n_0^{(nt)} + n_1^{(nt)}(1 - h(e_p^{(nt)})) - \log_2 \frac{2}{(\alpha_5 \alpha_6)^2}, \end{aligned} \quad (34)$$

where $\nu_2 = 2\alpha_1 + \alpha_2 + \alpha_3$ and $\nu_3 = 2\alpha_4 + \alpha_5 + \alpha_6$.

Combing Eqs.(31-34), the final secret key from both the triggered and nontriggered events is said to be ε_{sec} -secret if its length ℓ_B is chosen by

$$\begin{aligned} \ell_B &\geq n_0^{(t)} + n_0^{(nt)} + n_1^{(t)}(1 - h(e_p^{(t)})) + n_1^{(nt)}(1 - h(e_p^{(nt)})) \\ &\quad - \lambda_{EC}^{(t)} - \lambda_{EC}^{(nt)} - \log_2 \frac{2}{\nu_1^2} - \log_2 \frac{4}{\alpha_p^2}, \end{aligned} \quad (35)$$

with

$$\begin{aligned} \varepsilon_{\text{sec}} &= \nu + \bar{\nu} + \epsilon_{\text{pe}} \\ &= \nu_1 + 2(2\alpha_1 + \alpha_2 + \alpha_3) + 2\alpha_4 + \alpha_5 + \alpha_6 + \bar{\nu} + \epsilon_{\text{pe}}, \\ \alpha_p &= \alpha_2 \alpha_3 \alpha_5 \alpha_6 \varepsilon_{\text{cor}} \bar{\nu}, \end{aligned} \quad (36)$$

where ϵ_{pe} is the failure probability of estimating the single-photon yield and error rate.

For evaluation, we set each error term in Eq.(38) to a common value ε and let $\epsilon_{\text{pe}} = \varepsilon$. Therefore, the secrecy for the key obtained from both the triggered events and nontriggered events is $\varepsilon_{\text{sec}} = 15\varepsilon$. Then, considering the

TABLE I: List of experimental parameters for simulations: α is the loss coefficient of the fiber, f_{EC} is the error-correction efficiency, η_B is the detection efficiency of Bob's detectors, e_d is the error rate due to optical errors, which is the probability that a photon sent from Alice hits the erroneous detector, p_d is the background dark-count rate of Bob's detectors, η_A and d_A are the detection efficiency and dark count rate of Alice's detector, respectively.

α (dB/km)	f_{EC}	η_B	e_d	p_d	d_A	η_A
0.20	1.16	0.1	0.005	$6 \times 10^{(-7)}$	10^{-6}	0.5

bounds of single-photon yield and error rate given in the previous subsections, ℓ_B can be obtained as the following

$$\begin{aligned} \ell_B &= \min_x \{ N(1 - p_{\text{pe}}) Q^{(\text{nt})} [(\delta_0 x + x - \frac{\chi_0}{Q^{(\text{nt})}}) \\ &\quad + (\delta_1 \zeta(x) - \frac{\chi_1}{Q^{(\text{nt})}})(1 - h(e_p^{(t)})) + \zeta(x)(1 - h(e_p^{(\text{nt})})) \} \\ &\quad - N(1 - p_{\text{pe}}) Q^{(t)} f_{\text{EC}} h(E^{(t)}) \\ &\quad - N(1 - p_{\text{pe}}) Q^{(\text{nt})} f_{\text{EC}} h(E^{(\text{nt})}) \\ &\quad - 2 \log_2 \frac{15}{\varepsilon_{\text{sec}}} - 1 - 10 \log_2 \frac{15}{\varepsilon_{\text{sec}}} - \log_2 \frac{4}{\varepsilon_{\text{cor}}}, \end{aligned} \quad (37)$$

where

$$\begin{aligned} \chi_i &= \sqrt{\frac{\delta_i p_i \ln(15/\varepsilon_{\text{sec}})}{2N p_{\text{pe}}}} \quad \text{with } i = 0 \text{ or } 1, \\ e_p^{(t)} &= g(\mathcal{W}_t(x)), \\ e_p^{(\text{nt})} &= g(\mathcal{W}_{\text{nt}}(x)). \end{aligned} \quad (38)$$

In Eqs.(37) and (38), the minimum is numerically taken over the range $0 \leq x \leq \min\{2E^{(t)}\delta/\delta_0, 2E^{(\text{nt})}\}$ [48].

To conclude, the length of the final secret key can be given as $\ell = \max\{\ell_T, \ell_B\}$.

V. NUMERICAL SIMULATION

In this section, by assuming a fiber-based channel model, we numerically show the performance of our protocol with finite-length key. Let $\eta_c = 10^{-\alpha L/10}$ being the fiber transmission with $\alpha = 0.2$ dB/km the attenuation coefficient, η_B the quantum efficiency of Bob's detectors and $\eta \equiv \eta_c \eta_B$. For better comparison, we borrow experimental parameters from Ref. [37], which assumes that Bob uses an active measurement setup with two single-photon detectors with total detection efficiency $\eta_B = 0.1$ and dark-count probability $p_d = 6 \times 10^{-7}$. On the sender's side, we assume Alice uses a SPDCS and a typical silicon avalanche photodiode as threshold detector with $d_A = 10^{-6}$ and $\eta_A = 0.5$. The numerical parameters used are listed in Table I.

For the average overall gain $Q^{(t)}$ and $Q^{(\text{nt})}$, also the average quantum bit error rate (QBER) $E^{(t)}$ and $E^{(\text{nt})}$, they can be directly measured in the experiment. In this paper, for simulation purpose, we neglect the finite size effect in the calculation of the average overall gain and QBER. Then, according to the channel model, it is given

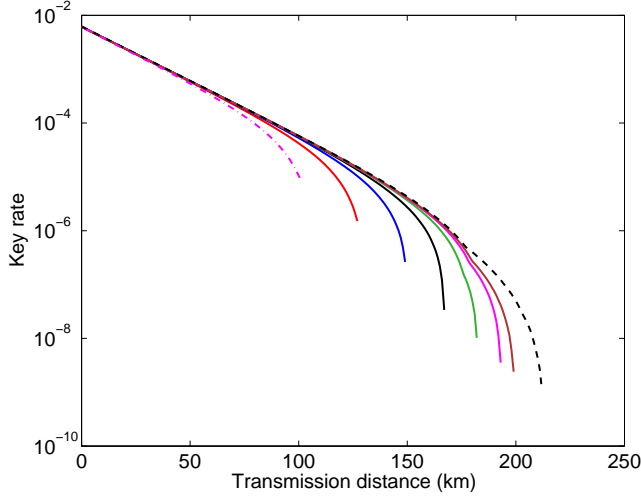


FIG. 1: (Color online) Secret key rate vs transmission distance. The secret key rates from left to right are numerically optimized for fixed number of total pulses from the SPDC process $N = 10^j$ with $j = 9, 10, \dots, 15$. The dashed curve denotes to the asymptotic secret key rate calculated from Eqs.(9)-(14) in Ref. [48], i.e., the key rate of the AYKI protocol with keys of infinite length; The intensity μ of the SPDCS and the probability p_{pe} of sample events in the total pulses are numerically chosen to be optimal for different transmission distances.

that

$$\begin{aligned}
 Q^{(t)} &= \sum_{n=0}^{\infty} p_n \gamma_n [1 - (1 - \eta)^n (1 - p_d)^2], \\
 Q^{(nt)} &= \sum_{n=0}^{\infty} p_n (1 - \gamma_n) [1 - (1 - \eta)^n (1 - p_d)^2], \\
 E^{(t)} &= \frac{1}{2Q^{(t)}} \sum_{n=0}^{\infty} p_n \gamma_n \{1 - (1 - \eta)^n (1 - p_d)^2 \\
 &\quad - (1 - p_d)[(1 - \eta e_d)^n - (1 - \eta + \eta e_d)^n]\}, \\
 E^{(nt)} &= \frac{1}{2Q^{(nt)}} \sum_{n=0}^{\infty} p_n (1 - \gamma_n) \{1 - (1 - \eta)^n (1 - p_d)^2 \\
 &\quad - (1 - p_d)[(1 - \eta e_d)^n - (1 - \eta + \eta e_d)^n]\}, \quad (39)
 \end{aligned}$$

with $p_n = \frac{\mu^n}{(1+\mu)^{n+1}}$ and $\gamma_n = 1 - (1 - d_A)(1 - \eta_A)^n$. The summations in Eq.(39) can be solved mathematically. However, for simplicity, we do not give their expressions here.

In our simulations, the key's secrecy ε_{sec} and correctness ε_{cor} are set to be 10^{-10} and 10^{-12} , respectively. For the estimation of the phase error rate, we assume $n = l \geq 125$. Note that the analysis in Ref. [33] is based on the QKD protocol with an ideal single-photon source. However, in our paper, a practical SPDCS is used in our protocol, which is within reach of current technology. Hence, the sifted key bits n should be replaced by the fraction bits of the single-photon contribution, that is, $n = N(1 - p_{pe})Q_1$. Here, Q_1 represents the gain from the single-photon detections. Then, for the estimate of phase error rate in Eqs.(30) and (37), i.e., $e_p^{(t)}$ and $e_p^{(nt)}$, we

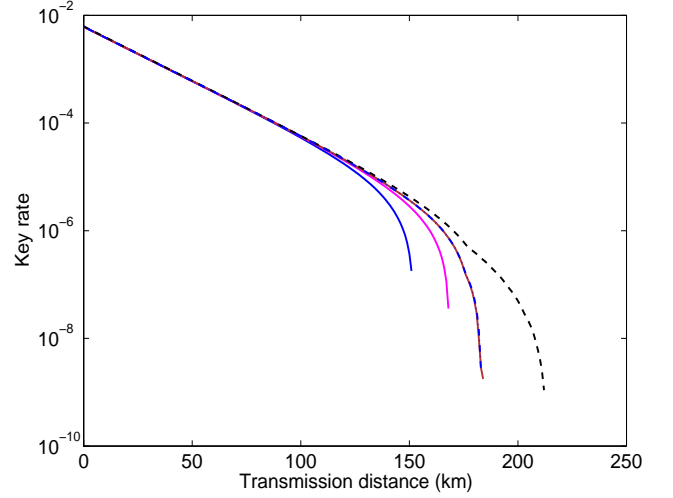


FIG. 2: (Color online) Secret key rate vs transmission distance. N is fixed to be 10^{13} . For different $p_{pe} = 0.01, 0.1, 0.9$, the solid lines (from left to right) are still plotted with intensity μ chosen optimally for different transmission distances. The dash-dotted curve denotes to the secret key rate when $p_{pe} = 0.96$ and the dashed curve still corresponds to the asymptotic secret key rate.

shall set their n be $N(1 - p_{pe})Q_1^{(t)}$ and $N(1 - p_{pe})Q_1^{(nt)}$, respectively. Likewise, the number of sample bits used for parameter estimation, i.e., $l^{(t)}$ and $l^{(nt)}$, are set to be $Np_{pe}Q_1^{(t)}$ and $Np_{pe}Q_1^{(nt)}$, respectively. Under these conditions, we apply an optimization about the secret key rate $R = \ell/(2N)$ over $\{x, \mu, p_{pe}\}$ given that the set $\{\varepsilon_{sec}, \varepsilon_{cor}, e_d, \eta_B, p_d, d_A, \eta_A, f_{EC}, Q^{(t)}, Q^{(nt)}, E^{(t)}, E^{(nt)}\}$ is fixed.

In Fig.1, the numerically optimized secret key rates from left to right are obtained by Eqs. (37) and (38) for a fixed number of total pulses $N = 10^j$ with $j = 9, 10, \dots, 15$, respectively. It should be noted that, so as to reach the distance of 100 km, N should be at least 10^9 . When we consider the postprocessing block size n_X mentioned in Ref. [37], the least requirement corresponds to $n_X \geq N(1 - p_{pe})R \geq 10^6$, larger than the one with a WCS by Lim et al. [37]. But within the distance of 50 km for $N = 10^9$, the secret key rate calculated by our method can be higher than 5.397×10^{-4} , which is better than the one using a WCS (lower than 10^{-4} by Fig.1 of [37]). And when one fixes N to 10^{13} corresponding to a postprocessing block size of 10^9 , the maximal transmission distance can reach to 167 km, which is getting close to 180 km with the WCS under the same conditions. Most importantly, from Fig.1, one can find that the maximal transmission distance of our method for $N = 10^{13}, 10^{14}$ and 10^{15} can be longer than 182 km, which performs better than the case using WCS for a postprocessing block size of 10^9 .

In Fig.2, we also simulate the secret key rates for different probabilities of p_{pe} . Without loss of generality, when

we fix N to be 10^{13} , one can see that the smaller value of p_{pe} results a lower secret key generation rate. When p_{pe} is larger than 0.9 (e.g. $p_{pe} = 0.96$), the maximal transmission distance is almost unchanged, representing the optimality of p_{pe} at 0.9. And our simulation is likely to help experimentalists to improve the performance of their QKD experiments using SPDCS.

VI. CONCLUSION

In conclusion, we put forward a passive decoy-state protocol in the finite-size effect. For ε -secure secret keys with finite length, the bound for estimating the single-photon contributions, single-photon errors and the length of final keys are presented. From numerical simulations, we remark that the QKD using a SPDCS performs as well as that using WCS. Furthermore, we conclude that our passive decoy-state protocol with a finite-length key

can reach a higher secret transmission distance than that using WCS. And our protocol can certainly be considered as a choice for the practical experiment of QKD using SPDCS.

We notice that a recent study by Krapick et al. [59] proposed a kind of SPDCS with bright intensity, which can be applied in our passive decoy-state protocol. It will be attractive and interesting to analyze the performance of QKD using this source. We shall concentrate on this issue in future works.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the financial support from the National Basic Research Program of China (Grant No. 2013CB338002) and the National Natural Science Foundation of China (Grants No.11304397, No.61101137, No.61201239 and No. 61205118).

-
- [1] C. H. Bennett, G. Brassard, in Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175-179, (1984)
 - [2] H.-K. Lo, H. F. Chau, Science 283, 5410 (1999); P. W. Shor and J. Preskill Phys. Rev. Lett. 85, 441 (2000).
 - [3] D. Gottesman, H.-K. Lo, Norbert Lükenhaus, and John Preskill, Quant. Inf. Comp. 4, 325 (2004)
 - [4] M. Tomamichel and R. Renner, Phys. Rev. Lett. 106, 110506 (2011).
 - [5] S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, et al., Opt. Lett. 37, 1008 (2012).
 - [6] X. S. Ma et al., Nature 489, 269 (2012).
 - [7] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, Nat. Commun. 4 (2013).
 - [8] J.-Y. Wang et al., Nat. Photonics 7, 387 (2013).
 - [9] B. Frohlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, Nature 501, 69 (2013).
 - [10] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics 81, 1301 (2009).
 - [11] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K. Lo. Phys. Rev. A 78, 042333 (2008).
 - [12] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics 4, 686 (2010).
 - [13] H. W. Li et al., Phys. Rev. A 84, 062308 (2011).
 - [14] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
 - [15] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. 105, 070501 (2010);
 - [16] M. Pawłowski and N. Brunner, Phys. Rev. A 84, 010302 (2011).
 - [17] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
 - [18] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).
 - [19] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A 85, 042307 (2012).
 - [20] X. F. Ma and M. Razavi, Phys. Rev. A 86, 062319 (2012).
 - [21] C. Zhou, W. S. Bao, W. Chen, H. W. Li, Z. Q. Yin, Y. Wang, and Z. F. Han, Phys. Rev. A 88, 052333 (2013).
 - [22] M. Hayashi, Phys. Rev. A. 76, 012329 (2007); J. Hasegawa, M. Hayashi, T. Hiroshima and A. Tomita, preprint arXiv:0707.3541 (2007).
 - [23] R. Cai and V. Scarani, New J. Phys. 11, 045024 (2009).
 - [24] H.-W. Li, Y.-B. Zhao, Z.-Q. Yin, S. Wang, Z.-F. Han, W.-S. Bao, and G.-C. Guo, Opt. Commun. 282, 4162 (2009).
 - [25] T. T. Song, J. Zhang, S. J. Qin and Q. Y. Wen, Quantum Inf. Comput. 11, 374-389 (2011).
 - [26] R. D. Somma and R. J. Hughes, Phys. Rev. A. 87, 062330 (2013).
 - [27] R. Renner, Ph.D. thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005, *quant-ph/0512258*; R. Renner, Int. J. Quantum Inf. 6, 1 (2008).
 - [28] V. Scarani and R. Renner, in Theory of Quantum Computation, Communication, and Cryptography, edited by Y. Kawano and M. Mosca (Springer, Berlin/Heidelberg, 2008), Vol. 5106 of Lecture Notes in Computer Science, pp. 83C95.
 - [29] V. Scarani and R. Renner, Phys. Rev. Lett. 100, 200501 (2008).
 - [30] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. 102, 020504 (2009).
 - [31] S. Bratzik, M. Mertz, H. Kampermann, and D. Bruß, Phys. Rev. A 83, 022330 (2011).
 - [32] N.H.Y. Ng, M. Berta, and S. Wehner, Phys. Rev. A 86, 042315 (2012).
 - [33] M. Hayashi and T. Tsurumaru, New. J. Phys. 14 (2012).
 - [34] M. Hayashi and R. Nakayama, arXiv:1302.4139v3 (2013).
 - [35] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. 3, 634 (2012).
 - [36] M. Mertz, H. Kampermann, S. Bratzik, and D. Bruß, Phys. Rev. A 87, 012315 (2013).
 - [37] C.C.W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A 89, 022307 (2014).
 - [38] M. Curty, F.H. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.K. Lo, Nat. Commun. 5, 3732 (2014).
 - [39] Y. Wang, W.S. Bao, H.W. Li, C. Zhou, and Y. Li, Phys.

- Rev. A 88, 052322 (2013).
- [40] M. Mafu, K. Garapo, and F. Petruccione, Phys. Rev. A 88, 062306 (2013).
 - [41] A. Vitanov, F. Dupuis, M. Tomamichel and R. Renner, IEEE Trans. Inf. Theory 59, 2603-2612 (2013).
 - [42] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. 85, 1330 (2000).
 - [43] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
 - [44] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
 - [45] X.-B. Wang, Phys. Rev. Lett. 94, 230503 (2005).
 - [46] M. Curty, X. Ma, B. Qi, and T. Moroder, Phys. Rev. A 81, 022310 (2010).
 - [47] W. Maurer and C. Silberhorn, Phys. Rev. A 75, 050305(R) (2007).
 - [48] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. 99, 180503 (2007).
 - [49] X. Ma and H.-K. Lo, New J. Phys. 10, 073018 (2008).
 - [50] M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, Opt. Lett. 34, 3238 (2009).
 - [51] Y. G. Tan and Q. Y. Cai, Int. J. Quantum Inf. 9, 903 (2011).
 - [52] R. Renner, Nature Physics 3, 645 (2007).
 - [53] R. J. Serfling, The Annals of Statistics, 2(1):39C48, (1974).
 - [54] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, Commun. Math. Phys. 328, 251 (2014).
 - [55] N. Lütkenhaus, Phys. Rev. A 61, 052304 (2000).
 - [56] X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A 72, 012326 (2005).
 - [57] J.-Z. Hu and X.-B. Wang, Phys. Rev. A 82, 012331 (2010).
 - [58] C.-H. F. Fung, X. Ma and H. F. Chau, Phys. Rev. A 81, 012318 (2010).
 - [59] S. Krapick, M.S. Stefszky, M. Jachura, B. Brecht, M. Avenhaus, and C. Silberhorn, Phys. Rev. A 89, 012329 (2014).